Wikileaks and the Protect-IP Act: A New Public-Private Threat to the Internet Commons

WikiLeaks and the PROTECT-IP Act: A New Public-Private Threat to the Internet Commons

Yochai Benkler

Abstract: The WikiLeaks affair and proposed copyright bills introduced in the Senate are evidence of a new, extralegal path of attack aimed at preventing access and disrupting the payment systems and advertising of targeted sites. In this model, the attacker may be a government agency seeking to circumvent constitutional constraints on its power or a private company trying to enforce its interests beyond those afforded by procedural or substantive safeguards in the law. The vector of attack runs through the targeted site's critical service providers, disrupting technical services, such as Domain Name System service, cloud storage, or search capabilities; and business-related services, such as payment systems or advertising. The characteristics that make this type of attack new are that it targets an entire site, rather than aiming for removal or exclusion of specific offending materials; operates through denial of business and financial systems, in addition to targeting technical systems; and systematically harnesses extralegal pressure to achieve results beyond what law would provide or even permit.

YOCHAI BENKLER is the Berkman Professor of Entrepreneurial Legal Studies at Harvard University, where he also serves as Faculty Co-director of the Berkman Center for Internet and Society. His publications include "The Commons as a Neglected Factor of Information Policy," Telecommunications Policy Research Conference (1998); "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access," *Federal Communications Law Journal* (2000); and *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (2006).

In December 2010, a website that the Pentagon had described in 2008 as dedicated "to expos[ing] unethical practices, illegal behavior, and wrongdoing within corrupt corporations and oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa, and the Middle East," and that in 2009 had received the Amnesty International New Media Award for reporting on extrajudicial killings in Kenya, came under a multisystem denial-of-service attack intended to prevent it from disseminating information. The attacks combined a large-scale technical distributed-denial-of-service (DDoS) attack with new patterns of attack aimed to deny Domain Name System (DNS) service and cloud-storage facilities, disrupt payment systems services, and disable an iPhone app designed to display the site's content.

The site was WikiLeaks. The attackers ranged from unidentified DDoS attackers to Senator Joseph Lieberman and, more opaquely, the Obama admin-

istration. The latter attack is of particular interest here, having entailed an extralegal public-private partnership between politicians gunning to limit access to the site, functioning in a state constrained by the First Amendment, and private firms offering critical functionalities to the site – DNS, cloud storage, and payments, in particular – that were not similarly constrained by law from denying service to the offending site. The mechanism coupled a legally insufficient but publicly salient insinuation of illegality and dangerousness with a legal void. By publicly stating or implying that WikiLeaks had acted unlawfully, the attackers pressured firms skittish about their public image to cut off their services to WikiLeaks. The inapplicability of constitutional constraints to nonstate actors created the legal void, permitting firms to deny services to WikiLeaks. This, in turn, allowed them to obtain results (for the state) that the state is prohibited by law from pursuing directly. The range of systems affected by the attack was also new: in addition to disrupting technical service providers – which had been familiar targets since efforts to control the Net began in the 1990s – the attack expanded to include payment systems.

This pattern of attack is not an aberration. One need only observe its similarities to current efforts by the copyright industries to shut down sites that challenge their business models. This objective was laid out most explicitly in the first draft of the Combating Online Infringements and Counterfeits Act (COICA)[1] that was introduced in September 2010, and a powerful version of it remains in the present version of the bill, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT-IP Act) of 2011.[2] The COICA/PROTECT-IP approach, which replicates the dynamics of the WikiLeaks attack, endeavors to create a relatively procedure-free context for designating sites as legally suspect actors, while making critical service providers immune from responsibility for any action they take by denying technical, payment, and business process systems to targeted sites. Together, these elements form the basis for extralegal attacks on critical services, thereby creating a shortcut to shutting down allegedly offending sites. The insinuation of illegality creates the basis for public pressure on the service providers to deny service; immunity replicates the legal void that allows service-provider action well beyond anything a court would have ordered.

Combining denial-of-payment systems with the use of extrajudicial mechanisms and private party enforcement appears to extend basic techniques developed in the war on terrorism into the civilian domain. It represents a new threat not only to the networked commons, but to the very foundations of the rule of law in the United States.

On November 28, 2010, WikiLeaks, in cooperation with *The New York Times*, the *Guardian*, *Der Spiegel*, *Le Monde*, and *El País*, began to release a set of leaked U.S. embassy cables. The following is a condensed version of a detailed and fully documented event study of the response to that disclosure.[3] WikiLeaks, a site dedicated to making materials leaked by whistleblowers public, had published a series of items from the Pentagon and the State Department between April and November 2010. The first release, a video showing American helicopters shooting a Reuters photographer and his driver, exposed previously hidden collateral damage incurred in the pursuit of insurgents. The video was followed by the release of thousands of war logs in which field commanders described conditions on the ground in Afghanistan and Iraq. The disclosures were initially described by the administration as highly

damaging to the security of troops and human rights workers, but as time passed, formal Pentagon assessments sent to Congress suggested that no such harm had occurred.[4] On November 28, WikiLeaks and its traditional-media partners began to release documents selected from a cache of about 250,000 classified cables that U.S. embassies around the world had sent to the State Department. In late November and December they published, in redacted form, a few hundred of these cables. WikiLeaks's decision to publish the materials, including when and how they were published, was protected by First Amendment law. Indeed, precedents established at least as far back as the *Pentagon Papers* case support the proposition that a U.S. court would not have ordered removal or suppression of the documents, nor would it have accepted a criminal prosecution of WikiLeaks or any of its editors and writers.[5]

Despite the constitutional privilege that allowed WikiLeaks to publish the leaked documents, American political figures widely denounced the disclosures. Moreover, critics appeared to blame only WikiLeaks, even though traditional outlets such as *The New York Times* were providing access to the same cables, and in the same form. The most effective critic, Chairman of the Senate Homeland Security Committee Senator Joseph Lieberman, urged companies providing services to WikiLeaks to cease doing so. Senator Lieberman issued his call on December 1, 2010, following a well-crafted letter from the State Department to WikiLeaks sent November 27, 2010. That letter did not take the legally indefensible position that WikiLeaks itself had broken the law. Instead, it correctly asserted that the law had been broken (by someone), insinuating that WikiLeaks was the offending party. Not surprisingly, implicated service providers were among those who misread the letter. In a critical move, PayPal discontinued its service to WikiLeaks; a vice president of the firm, commenting publicly, pointed to the November 27 letter, not to Senator Lieberman's call, as the reason that PayPal believed WikiLeaks had broken the law, thus triggering the firm's decision to stop payment service to WikiLeaks.[6] The State Department letter was complemented by a series of public statements that tried to frame WikiLeaks's embassy cable release as international terrorism. Secretary of State Hillary Clinton called the release of the cables "an attack on the international community." Vice President Joseph Biden explicitly stated that Julian Assange, the founder of WikiLeaks, was "more like a high-tech terrorist than the Pentagon Papers." Senator Dianne Feinstein wrote a *Wall Street Journal* editorial calling for Assange's prosecution under the Espionage Act. Some right-wing politicians simply called for his assassination on the model of U.S. targeted killings against Taliban and Al Qaeda leaders.[7]

Against the backdrop of this massive public campaign against WikiLeaks, Senator Lieberman's December 1 public appeal was immediately followed by a series of service denials:

- December 1: *Storage*. Amazon removes WikiLeaks materials from its cloud-storage facility.
  - –*Countermeasure:* WikiLeaks moves storage to OVH in France.
- December 2: *DNS*. EveryDNS, the DNS registrar serving the WikiLeaks.org domain, stops pointing the domain name to WikiLeaks's server.
  - –*Countermeasure:* WikiLeaks uses numeric IP addresses updated through Twitter and begins to rely more heavily on WikiLeaks.ch DNS as well as on mirroring by various volunteers throughout the Net.

- December 3, 5: *Storage*. French Minister of Industry Eric Besson calls on OVH to cease providing storage; by December 5, OVH removes WikiLeaks content.
  - *Countermeasure:* WikiLeaks moves again, to Sweden, initially to the servers of the Pirate Party, a Swedish political party, and later to a Swedish storage provider.
- December 4: *Payment systems*. PayPal stops processing donations for WikiLeaks, cutting off a major source of funding. A vice president of PayPal points to the State Department's November 27 letter to WikiLeaks as the reason PayPal concluded that WikiLeaks was acting illegally and terminated service.
  - *Countermeasure:* No effective response. WikiLeaks loses substantial revenue as PayPal ceases to process donations. Loss of revenue continues with the credit card stoppages that follow.
- December 6: *Payment systems*. MasterCard stops servicing WikiLeaks. The Swiss Postal Bank closes Julian Assange's personal account with the Swiss bank for his failure to provide an adequate address.
- December 7: *Payment systems*. Visa joins MasterCard. Bank of America discontinues services ten days later.
- December 20: *App store*. Apple removes a third-party app created to allow iPhone users to access and search WikiLeaks embassy cables.
  - *Countermeasure:* WikiLeaks has no possible recourse. However, apps for the Android smartphone were not removed.

None of these companies was compelled by legal order to deny services to WikiLeaks. Indeed, under First Amendment law, it would have been impossible for the government or anyone else to obtain such an order. That aspect of U.S. constitutional law justifies describing this set of events as an *attack* on WikiLeaks. Put differently, the service denials to WikiLeaks were the result of an effort by the government to shut down the site irrespective of the fact that the law prohibited the government from doing so. In private conversations, individuals within and close to the administration emphatically denied any back-channel communications threatening or cajoling the companies. These claims seem plausible, and for purposes of analysis here, I consider them to be true. My claim, however, is based not on intent or the likelihood of conspiracy, but on effect. A public media campaign against WikiLeaks, led by top administration figures and some of the most senior politicians in the president's party, triggered vigilante actions by corporations that, unfettered by the laws constraining public-sector responses, likely saw themselves as acting in the national interest as they degraded the site's capabilities. Regardless of how its actions were perceived, WikiLeaks was engaged in classic fourth-estate functions at the core of freedom-of-the-press protections. In order to guard against similar outcomes in the future, it is important to understand and correctly characterize the events against the site as an attack on an important practice in the networked commons.

From a technical perspective, the attack was largely unsuccessful. The site proved enormously robust, using the core modes of networked resilience, namely, redundancy and decentralized cooperation. When WikiLeaks.org was denied DNS service, the site used a range of numeric IP addresses circulated on blogs and Twitter. It moved through a series of non-U.S. domains, the most important of which was the Swiss domain name WikiLeaks.ch. The Swiss DNS service provider, Switch, refused to capitulate to pressures to cease service to WikiLeaks. When cloud storage was denied in the United States, the site

moved first to France, where service was again denied under pressure from the French government, and then to Sweden. Moreover, thousands of mirror sites sprang up to permit access to the documents that had been released up to that point. However, where the system was not Internet based, as in the case of the iPhone app, it was impossible to replace. Nonetheless, the relative insignificance of the app, as long as an open Internet alternative existed, minimized the importance of that pathway. However, the fact that the WikiLeaks app was not easily replaceable provides an important indication of how vulnerable information is when available only over an iPhone or iPad-accessed network; the open Internet, by contrast, is robust.

Targeting WikiLeaks's business systems proved much more successful as a line of attack. WikiLeaks, which depends on donations from supporters to fund its operations, apparently lost 80 to 90 percent of its revenue stream in the first two months of the attack, and only gradually was able to create a set of proxies for receiving donations.[8] As was the case with the iPhone app, in the absence of a competitive market to offer significant redundant pathways for payment systems, persuading two or three companies to deny service was sufficient to severely hamper the site's payment operations. Whether a targeted site is a nonprofit dependent on donations or a for-profit or low-profit enterprise funded by transactions or advertising, an attack on the business systems a site depends on for financing appears harder to avert. This particular attack on payment systems seems to derive from the war-on-terror rhetoric applied to WikiLeaks as well as from a decade-old program established to compel payment and financial services firms to shut off funds flowing to terrorist organizations.[9]

The attack on WikiLeaks largely failed to achieve its goals. If it was aimed to prevent people around the world from accessing the leaked materials, it failed. The materials were made available on both distributed mirror sites and the sites of traditional media partners, whose public visibility seems to have made them invulnerable to the kind of informal, extralegal pressure that worked to deny service to WikiLeaks. If it was aimed to discredit the reports, it clearly failed here because WikiLeaks's partnership with traditional media helped raise visibility and add credibility to the documents. The technical aspect of the attack failed almost entirely: redundancy and the ability to move from one country to another allowed for robust storage, and the creation of thousands of mirror sites by individuals around the world made DDoS and DNS attacks ineffective.

Moreover, not all firms folded as easily as Amazon, PayPal, MasterCard, and Visa. Refusing to follow the U.S.-based EveryDNS, the Swiss DNS registrar continued to point to WikiLeaks.ch. Twitter declined to respond to document requests until subject to subpoena. Google did not remove related apps from the Android system or drop WikiLeaks results from its search engine. The success of an attack that relies on public pressure and a legal void in which to act depends on service providers' concern about being perceived as helping the targeted site; this concern must outweigh the providers' interest in maintaining their image as providers of robust, incorruptible services to the Internet-using public. Thus, the new form of informal, extralegal attack can be only partially effective if not all service providers are on board. Nonetheless, the denial of payment systems greatly affected WikiLeaks's cash flow and was likely the most effective and dangerous aspect of the attack.

This new pattern of attack (a) targeted an entire site; (b) was carried out through

denial of service by commercial service providers of critical technical and business capabilities; and (c) circumvented constitutional protections by creating an extralegal public-private partnership for censorship, using the inapplicability of constitutional limitations to private companies together with the relatively loose regulation of the standard-form contracts that govern the relations between service providers and their customers.

The WikiLeaks affair might properly have been dismissed as a one-off set of events if not for a similarly structured attack at the center of copyright legislation introduced in the Senate since late 2010. The PROTECT-IP Act is the most recent iteration of the U.S. copyright industries' seventeen-year-long drive to enlist various intermediaries and service providers of networked facilities to enforce their rights through law and public policy.[10] Beginning in the Clinton White House with a 1995 white paper[11] and culminating with the Digital Millennium Copyright Act (DMCA) of 1998,[12] the industries sought to create a set of liabilities that would lead Internet service providers (ISPs) and Web-hosting companies to remove infringing materials. The safe harbor notice and takedown procedures adopted in the DMCA represented the settlement of the first half-decade of policymaking in this field. Under these provisions, pure telecommunications carriers were excluded from the requirements of policing content. Providers of caching, Web-hosting, and search engines and Web directories were required to have a procedure in place for receiving notices regarding specific offending materials, and for taking down those materials; but they were not required to search out such content themselves or to block entire sites.

The following decade witnessed a legislative stalemate. On the one hand, the content industries hoped to expand control over materials on the Net in order to preserve and increase their revenues. On the other hand, a coalition of computer, software, and communications businesses that profited from the free flow of information and cultural goods online, together with civil society organizations aiming to preserve a space for a cultural commons, was concerned that efforts to impose controls would hamper the open, creative, participatory structure of the networked environment. While Republicans seemed less responsive to pressures from Hollywood, since 2006, Democrats controlling the Senate have pushed through a slate of laws designed to implement the Motion Picture Association of America's long-standing agenda. Most pertinent are the Prioritizing Resources and Organization for Intellectual Property Act (PRO-IP Act) of 2008, which created an IP czar in the White House and funded additional resources for criminal copyright enforcement,[13] and provisions in the Higher Education Opportunity Act of 2008[14] that required colleges to redesign their networks and develop offerings to protect the interests of Hollywood and the recording industry against their students. These laws include the two main elements of the bills currently under consideration: that is, they expanded the involvement of criminal enforcement authorities in what was traditionally an area of private commercial law, and they used state leverage to harness private platform providers to enforce the interests of the copyright industries.

Unlike the settlement of the 1990s, the most recent set of bills targets not offending content, but offending sites. While the DMCA focused on specific documents that violated copyright, new legislation – in the same vein as the WikiLeaks case – seeks to take out entire sites, specifically those defined as primarily dedicated to unauthorized distribution of copyrighted ma-

terials. It also substantially expands the set of addressees who are enlisted to aid the content industries. In addition to carriers, caching providers, and Web-hosting companies (which, in today's incarnation, cover cloud-storage facilities), the new bills cover DNS providers, advertising providers, and payment systems such as PayPal or credit card companies. From a procedural standpoint, the newest bills combine elaborate procedures that would allow a court order against sites or domain names not subject to U.S. jurisdiction, with subtle efforts to harness and formalize the extralegal public-private partnership exhibited in the WikiLeaks affair.

Introduced in September 2010 as the first bill in this series, COICA clearly identified its target as sites that have "no demonstrably commercially significant purpose" other than providing access through downloading, streaming, or linking to unauthorized materials. The breadth of the definition, however, captures much more, including "providing access to any goods or services in violation of the Copyright Act" or enabling a violation. The more tightly defined target is only an example of this broader set. For instance, the broader definition would include a creative site dedicated to anime music videos that provides the underlying songs, as is so often the case with the genre, in full or in substantial part – even though the work is transformative. The breadth of coverage becomes clearer when considering the blacklist described below; developed by a copyright industry firm in June 2011, the list included Archive.org and distribution of basic technical tools such as BitTorrent. Here, my point is not to challenge the definition, but to outline the method of attack on sites targeted under the proposed law. COICA empowers the Attorney General – the same government division that the 2008 legislation bolstered – to enforce copyright through criminal law. If the Department of Justice determines that a given domain name is associated with a site that falls under COICA's definition of unlawful behavior, it can petition for a court order that would obligate DNS providers in the United States to stop resolving the domain; or, if the domain is registered with a DNS provider used by U.S. customers but not subject to U.S. jurisdiction, any U.S. service provider, ISPs in particular, is required to take reasonable measures to prevent the domain name from resolving to the offending site. Moreover, "financial transaction providers" are required to cease servicing the site and enforce their copyrights to prevent the site from using their logos. Finally, contextual advertising providers are required to stop serving ads to the site. The innovations embedded in COICA, relative to prior legislation, are (a) the introduction of a broad-based attack at the site level, rather than removal of discrete documents, and (b) the harnessing of payment systems and advertising to deny economic viability to the site. In this sense, COICA presaged the attack on WikiLeaks through the payment system.

Another element of the original COICA was its particularly crisp platform for extrajudicial enforcement. Although the original has since been abandoned in favor of more subtle versions, the original form crystallizes the intent of the later versions. In its initial form, COICA required the Attorney General to "maintain a public listing of domain names that, upon information and reasonable belief, the Department of Justice determines are dedicated to infringing activities but for which the Attorney General has not filed an action under this section." The threshold for designation as an offending site is extremely low: the Department of Justice simply must allege "upon information and reasonable belief" that a site is dedi-

cated to infringing activities. This provision invokes standard language used in litigation to indicate the minimum level of knowledge required for plaintiffs to sustain a complaint without subjecting themselves to sanctions; it suggests a generalized suspicion more than a real investigation. Once a site is blacklisted, DNS service providers, ISPs, payment system providers, and advertising providers are immunized from liability if they deny service to the site listed as offending.

Note that the technique employed here is similar to the one utilized in the attack on WikiLeaks. The evidentiary threshold for state designation of a "bad actor" is well below what would be necessary to obtain judicial approval of that actor's "badness." For this reason, the statute cannot demand that private third parties comply with the enforcement efforts. Nonetheless, this substandard designation of bad-actor status can be used to pressure private service providers into acquiescence. By combining the extrajudicial designation with immunity for firms that discontinue service to the targeted sites, the state increases the likelihood that private parties will comply. The promise of immunity both expresses the state's expectation that cooperative private providers will, in fact, act against the designated entities and minimizes the risk and cost of doing so. The immunity creates the legal void necessary for vigilante enforcement and shows that such actions are desirable to the state. By contrast, the targeted site owner's defense becomes expensive. The procedure proposed would not create a legal black hole: the Attorney General was required to create mechanisms for allowing site owners to challenge their blacklisting and to appeal an unfavorable decision to a reviewing court. But the process reverses the normal presumptions of innocence. The "bad actors" blacklist, coupled with immunity, allows the state to place substantial pressure on sites deemed offending without obtaining a judicial determination prior to triggering the attack.

What makes this form of attack so worrisome? Ultimately, cases will be subject to judicial review, and if the court rules that the closure is unjustified, it will be lifted. The problem is that this procedure allows for effective elimination of revenues and technical access for lengthy periods pending review. Because there is no specific order or process prior to blacklisting, a site can find itself technically inaccessible and unable to use payment systems or advertising. Unless a site can immediately reestablish a backup presence – that is, use the redundancy of multiple sites – it will likely be economically dead by the time it can challenge the listing.

In combination, COICA expands the vectors of attack to include payment systems and advertising networks and provides an extralegal avenue of attack without prior judicial approval that can be sustained for an unspecified period while administrative and judicial appeals are pending. These elements largely, though not completely, enable the state to circumvent or severely curtail the requirements of legality and the protections of procedure.

The Senate abandoned this explicit entanglement of the state in extralegal enforcement. The procedure was replaced by an immunity provision that created space for private enforcement of the multisystem attack. In the revised bill, the provision simply states: "No domain name registry, domain name registrar, financial transaction provider, or service that provides advertisements to Internet sites shall be liable to any person on account of any action described in this section voluntarily taken if the entity reasonably believes the Internet site is dedicated to infringing activities." The promise of

immunity creates a legal space for informal pressures on advertising and financial services firms to deny services to potentially offending sites. It effectively invites private entities to create blacklists of their own. Similar to the reasonable belief envisioned in the original COICA bill, those lists could provide the justification for blocking targeted sites.

The current draft of the PROTECT-IP Act replicates this latter approach. It expands on COICA by (a) creating a private right of action, which gives the copyright industries the power to initiate and enforce the attacks and (b) making the immunity provision applicable with regard to any site accused, rather than only non-U.S. sites, as was the case in COICA. Section 5 of the PROTECT-IP Act immunizes any service provider that in "good faith and based on credible evidence has a reasonable belief that the Internet site is an Internet site dedicated to infringing activities." This weak standard encourages the creation of industry-maintained blacklists to implicate sites allegedly engaged in offending activities. In turn, the legal immunity creates the perfect context for putting pressure on private infrastructure, payment systems, and advertising providers to deny service to the blacklisted sites. Not surprisingly, in June 2011, less than a month after publication of the most recent iteration of this type of immunity, the advertising firm GroupM, whose clients include Universal Music, Paramount, and Warner Bros., developed a blacklist of more than two thousand sites to which it would not serve ads.[15] The list reportedly includes sites that indeed appear to provide primarily illegal downloads as well as sites whose practices are clearly non-offending, such as Archive.org and a broad range of basic technology sites that could, in principle, be used for file sharing.[16] Reliance on such a list is unlikely to fail the "good faith and based on credible evidence" test of "reasonable belief" set out in the PROTECT-IP Act. This makes the blacklist, however imperfect, a base from which to launch an extrajudicial attack on payment systems, contextual advertising, DNS, and other technical services of these sites, entirely circumventing the procedural and substantive protections embedded in the Copyright Act and the federal rules of civil procedure.

The years 2010 and 2011 have witnessed the introduction of a new pattern of attack on controversial websites, one that involves both the state and major private actors in a public-private partnership formed to suppress offending content. WikiLeaks publishes content that is of primary concern to the state; the suppression of such content is prohibited by the First Amendment. The attack on the site sought to circumvent constitutional protections by applying informal pressure (which is not reviewable under the Constitution) to private actors (who were not subject to constitutional constraints) to further the state's objective of suppressing the publication of the materials in question. PROTECT-IP represents the inverse of this public-private partnership for censorship. Here, the interests are those of certain segments of the business community – the copyright industries – seeking to use the state to help harness other private actors to enforce their interests.

The elements common to both methods of attack are the denial of business and technical systems and the use of extralegal or very weakly legally constrained forms to designate the target of attack and to define the pattern of denial of service. The effect is to dispense with, or at least limit, the procedural and substantive protections afforded to targeted sites, and to degrade, if not completely prevent, the operations of the organizations that use the site. All this is achieved with

practically no need for judicial approval before the action, and with only relatively expensive and slow judicial review while the attack is ongoing.

The features of the attack are eerily familiar. They are the common characteristics of what was described as early as September 24, 2001, as "the financial front in the Global War on Terrorism."[17] The COICA model for designating bad actors to be blocked by private parties replicates the model developed in 2001 that allowed the Treasury Department to designate "blocked persons," a label that triggers obligations by banks and others to freeze assets and deny further use of payment systems. Administrative designation without need for judicial order, or weak-to-nonexistent procedural protection for targets, combined with the use of private business systems providers to execute the goals of the state is rooted in the model developed for the "war on terror" of the first decade of the 2000s. This model now appears to be introducing two new elements into much more mundane areas of social policy and organization. The first is the use of extrajudicial models for designating targets for attack. The second is harnessing private actors, in particular business and financial systems providers, to choke off fund flows to suspected organizations. Setting aside debates over whether those elements can be justified when the targets are suspected terrorist organizations, observing them metastasize to the civilian part of normal political and economic life in a democratic, networked society is extremely troubling and should be resisted – politically, legally, and technically.

ENDNOTES

1 Combating Online Infringements and Counterfeits Act of 2010, 111th Cong., 2nd. sess., September 20, 2010, S. 3804.

2 Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, 112th Cong., 1st. sess., May 12, 2011, S. 968.

3 The description is drawn from the extensively documented study, Yochai Benkler, "A Free Irresponsible Press: WikiLeaks and the Battle Over the Soul of the Networked Fourth Estate," *Harvard Civil Rights-Civil Liberties Law Review* 46 (2011). The study is also available at http://www.benkler.org/Benkler_Wikileaks_current.pdf.

4 Adam Levine, "Gates: WikiLeaks Don't Reveal Key Intel but Risks Remain," CNN.com, October 16, 2010, http://articles.cnn.com/2010-10-16/us/wikileaks.assessment_1_julian-assange-wikileaks-documents?_s=PM:US.

5 Benkler, "A Free Irresponsible Press," Part III.

6 According to a PayPal executive, "What happened is that on November 27th [the day before WikiLeaks began releasing cables] the State Department, the US government basically, wrote a letter saying that the WikiLeaks activities were deemed illegal in the United States. And so our policy group had to take a decision to suspend the account.…It was straightforward from our point of view"; Benkler, "A Free Irresponsible Press," n.146 – 148.

7 Ibid., Part II.A.

8 Ibid. This information is based on statements by Julian Assange in comments on an early draft of the article.

9 Patrick D. Buckley and Michael J. Meese, "The Financial Front in the Global War on Terrorism," U.S. Army War College Strategic Studies Institute, 2001, http://www.au.af.mil/au/awc/awcgate/army/usma_terrorists_finances.pdf.

10 There are many histories of this long battle. See James Boyle, *The Public Domain: Enclosing the Commons of the Mind* (New Haven, Conn.: Yale University Press, 2008); Jessica Litman, *Digital Copyright: Protecting Intellectual Property on the Internet* (Amherst, N.Y.: Prometheus Books, 2001); and Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven, Conn.: Yale University Press, 2006).

11 *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights* (Washington, D.C.: U.S. Department of Commerce, 1995).

12 Digital Millennium Copyright Act of 1998, Public Law 105-304, 105th Cong., 2nd. sess., October 28, 1998.

13 Prioritizing Resources and Organization for Intellectual Property Act of 2008, Public Law 110-403, 110th Cong., October 13, 2008.

14 The Higher Education Opportunity Act of 2008, Public Law 110-315, 110th Cong., August 14, 2008.

15 Mark Sweney, "WPP Blacklists More than 2,000 US Websites," *Guardian*, June 8, 2011, http://www.guardian.co.uk/media/2011/jun/08/wpp-groupm-sir-martin-sorrell.

16 "BitTorrent.com and Archive.org Blacklisted as Pirate Sites by Major Advertiser," TorrentFreak, October 6, 2011, http://torrentfreak.com/bittorrent-com-and-archive-org-blacklisted-as-pirate-sites-110610/.

17 Buckley and Meese, "The Financial Front in the Global War on Terrorism."